



المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

MSMEs
#safe_start_fortified_beginnings

Safe Start Fortified Beginnings



A cybersecurity guidebook
to help Bahrain's MSMEs
build resilience

Content

01

Introduction

02

The Strategic Importance of Cybersecurity for Micro, Small, and Medium Enterprises (MSMEs)

03

Global and Regional Cybersecurity Landscape

04

Bahrain's Economic Vision and Cybersecurity Readiness

05

How This Guidebook Supports MSMEs in Cybersecurity Readiness

06

Addressing Common Cybersecurity Misconceptions

07

Case Studies: Insights from Cybersecurity Incidents

08

Cyber Threats and Risk Assessment for MSMEs

09

Cybersecurity Maturity Model for MSMEs

10

The SMESEC Framework: 10 Strategic Steps to Strengthen Cybersecurity for Small and Medium Enterprises (SMEs)

11

Global Best Practices for MSME Cybersecurity

12

On an Ending Note "Empower Your Cybersecurity Journey"

01

INTRODUCTION

Micro, small, and medium enterprises (MSMEs) are vital to the global economy, but their increasing reliance on digital tools exposes them to growing cybersecurity risks. The World Economic Forum (WEF) has identified cyber threats as a top global business risk, while the International Telecommunication Union (ITU) stresses the need for a strong cybersecurity culture worldwide. MSMEs must adopt a strategic approach to cybersecurity—whether through high-level frameworks for medium enterprises or basic preparedness and cyber hygiene for micro and small businesses. Tailoring efforts to size and capacity helps ensure resilience, competitiveness, and long-term sustainability across the entire MSME spectrum.

As part of Bahrain's national effort to elevate cybersecurity readiness among MSMEs, the National Cyber Security Center (NCSC) launched the "Safe Start, Fortified Beginnings" campaign in May 2025. This guidebook was developed as a key component of that initiative, designed to empower MSMEs with accessible, practical, and strategic guidance to protect their digital assets. By addressing global risks, regional trends, and national goals, this guide serves as a trusted resource for MSMEs looking to build secure, resilient foundations in today's rapidly evolving digital economy.

02

The Strategic Importance of Cybersecurity for Micro, Small, and Medium Enterprises (MSMEs)

Globally, MSMEs account for over 90% of businesses and more than 60% of employment, underscoring their critical role in economic development. As these enterprises increasingly adopt digital technologies to enhance competitiveness and reach, they become more susceptible to cyber threats.

Recent studies highlight the growing cybersecurity challenges faced by MSMEs:



Rising Cyber Threats

In 2023 alone, there were over 400 million malware incidents, with MSMEs being prime targets due to their often-limited cybersecurity infrastructure.



Perception vs. Reality

Many MSMEs underestimate their risk exposure, believing they are too small to be targeted. However, cybercriminals often exploit smaller businesses as entry points to larger networks.



Economic Impact

Cyberattacks can lead to significant financial losses, operational disruptions, and reputational damage. For instance, phishing attacks have resulted in average losses of \$50,000 for affected MSMEs.

93%

Growing Sectors

(YoY)

of all registered businesses in the Kingdom of Bahrain are micro, small, and medium enterprises (MSMEs), making them pivotal to the Kingdom's economic landscape.

These enterprises are instrumental in:

Contributing to economic diversification

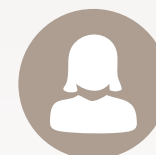
Generating employment

Driving innovation

Notably, about **81%** of these enterprises are Bahraini owned, with approximately:



39%
owned by youth



23%
owned by women

Reflecting a diverse and dynamic entrepreneurial ecosystem.

Top Economic Indicators

(YoY)



Inbound Tourism Flows
+24.7%



Value of Electronic Fund Transfers
+15.6%

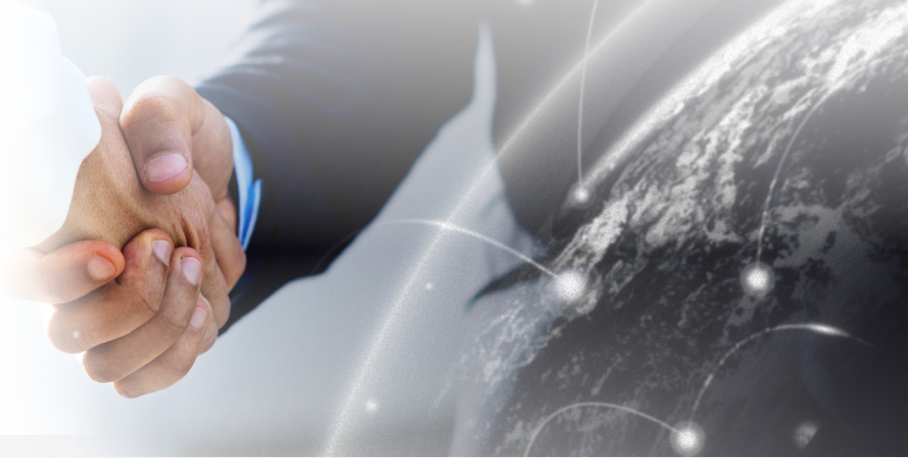


Value of POS & E-Commerce
+7.9%




Real Estate Transactions
+24.1%

Strategic Imperatives for MSMEs



Comprehensive cybersecurity strategies are necessary for micro, small, and medium enterprises (MSMEs) to protect operations and contribute to regional and global economic stability.



Incorporating cyber insurance into a broader cybersecurity strategy enhances risk mitigation efforts, supports business continuity, and builds trust in global markets.



By proactively addressing cybersecurity, MSMEs can safeguard their operations, protect customer data, and maintain trust in the digital marketplace.

Given the rising **challenges**, it's **imperative** for MSMEs to adopt a **strategic** approach to **cybersecurity**.

This guidebook will address these points at a high level, helping MSMEs:

01

Conduct risk assessment and management.

02

Foster cybersecurity awareness among employees.

03

Invest in security infrastructure.

04

Collaborate towards threat intelligence and best practices.

03

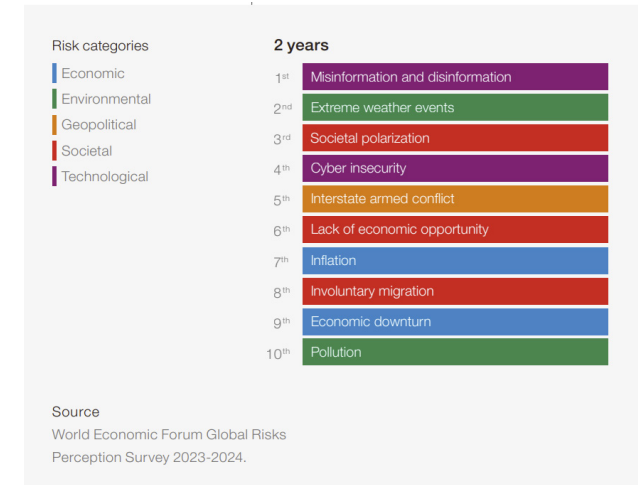
Global and Regional Cybersecurity Landscape

As micro, small, and medium enterprises (MSMEs) increasingly embrace digital transformation, they become more susceptible to cyber threats.

According to the World Economic Forum's (WEF) Global Cybersecurity Outlook 2025:



The World Economic Forum's (WEF) Global Risk Report highlights cybersecurity as one of the most critical economic threats.



35%

of small organizations perceive their **cyber resilience** as inadequate. This marks a significant increase compared to previous years, highlighting a growing vulnerability.

+60%

of small businesses that experience a **cyberattack** shut down within six months.

\$10 trillion

in annual global **cybercrime** costs is projected by the end of 2025, highlighting the scale of the threat.

+200%

increase in **ransomware** attacks was observed over the past year, targeting businesses of all sizes.

Key facts on the evolving cyber threat landscape worldwide:

80%

of **phishing attacks** are estimated to be AI-generated.

74%

of companies have reported a rise in **insider threats**.

72.7%

of organisations have experienced **ransomware**, the most prevalent cyber threat.

70%

of organizations are targeted by **business email compromise (BEC)**, making it the most common form of cyberattack.

88%

of all **cyber incidents** are attributed to **human errors**.

25%

of all cybersecurity incidents are linked to **BEC**, highlighting its significant impact across industries.

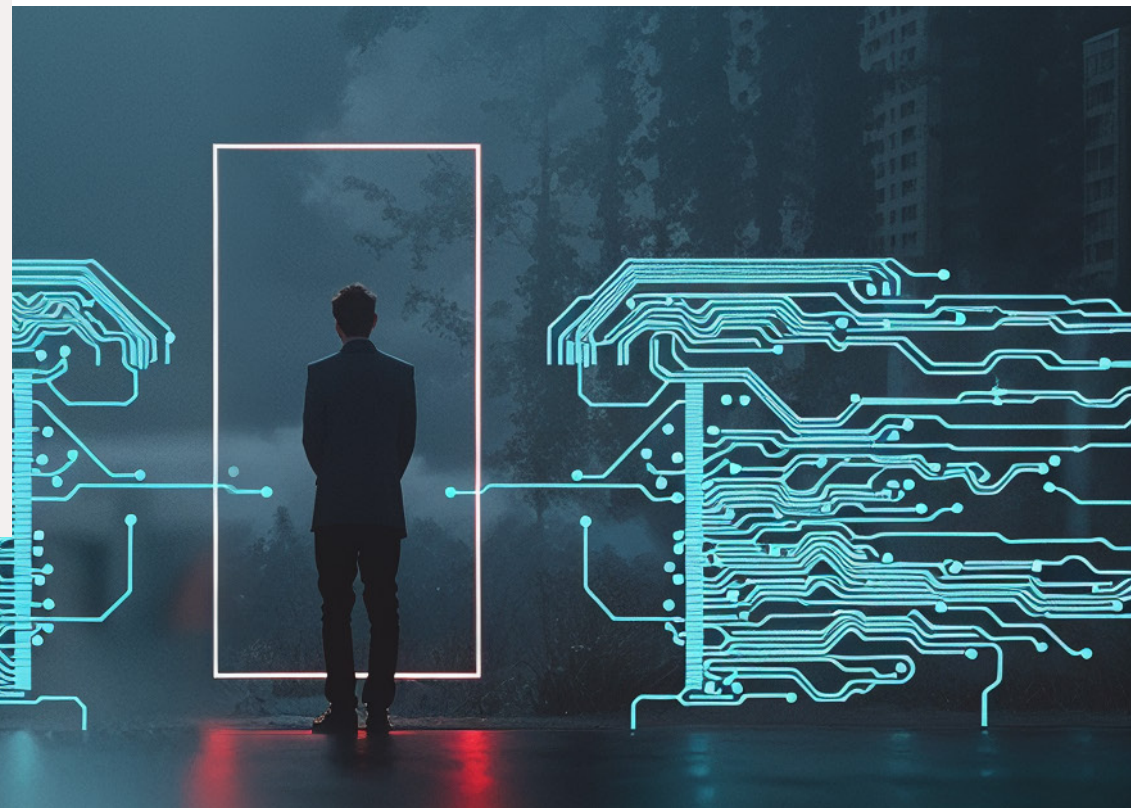
In the Gulf Cooperation Council (GCC) region:

250%

increase in **cyber threats** has been recorded over the past five years.

Critical sectors such as **finance, healthcare, and e-commerce** are particularly targeted.

This emphasizes the necessity for comprehensive cybersecurity strategies across all industries. Micro, small, and medium enterprises (MSMEs) must align with national cybersecurity strategies to safeguard their operations and contribute to regional economic stability.



04

Bahrain's Economic Vision and Cybersecurity Readiness

In line with Bahrain's Economic Vision 2030, which emphasizes a secure digital infrastructure as the foundation for sustainable economic growth, the National Cyber Security Center (NCSC) launched the "Safe Start, Fortified Beginnings" campaign in May 2025. The campaign aims to strengthen the cybersecurity posture of micro, small, and medium enterprises (MSMEs) by providing accessible resources and strategic cybersecurity guidance.

Cybersecurity serves as a key enabler of growth by:



Strengthening
the financial and
digital economy



Safeguarding
MSMEs' operations
and intellectual
property



Attracting foreign
investment
and fostering
innovation

**Bahrain's Economic Vision
2030 also highlights digital
transformation as a pillar
of economic growth.**



Strategic Benefits of Integrating Cybersecurity into Micro, Small, and Medium Enterprises (MSMEs) Operations:



Enhanced Customer Trust

Secure transactions and data protection build credibility and foster customer confidence.



Regulatory Compliance

Adhering to global and local cybersecurity laws ensures legal compliance and mitigates potential penalties.



Business Continuity

Proactive cybersecurity measures help prevent operational disruptions caused by cyber incidents.



Market Competitiveness

Demonstrating cyber resilience can attract partners and investors, providing a competitive edge.

MSMEs must integrate cybersecurity into their business strategies to fully align with Bahrain's national economic goals. By adopting a strategic approach to cybersecurity, MSMEs can:

Protect their assets

Maintain customer trust

Ensure sustainable growth in an increasingly digital economy



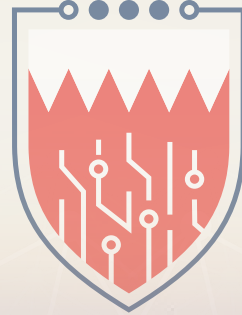
05

How This Guidebook Supports MSMEs in Cybersecurity Readiness

This guide is designed to assist micro, small, and medium enterprises (MSMEs) in navigating today's complex cybersecurity landscape by offering practical, scalable strategies aligned with global, regional, and national cybersecurity frameworks.

By understanding potential risks and adopting proactive measures, Bahraini MSMEs — regardless of size or sector — can strengthen their resilience, protect digital assets, maintain customer trust, and contribute to building a secure, thriving digital economy in line with Bahrain's Economic Vision 2030 aspirations.

This guidebook serves as a trusted resource, offering accessible guidance that empowers MSMEs to take informed, strategic action to secure their operations in an increasingly interconnected world.



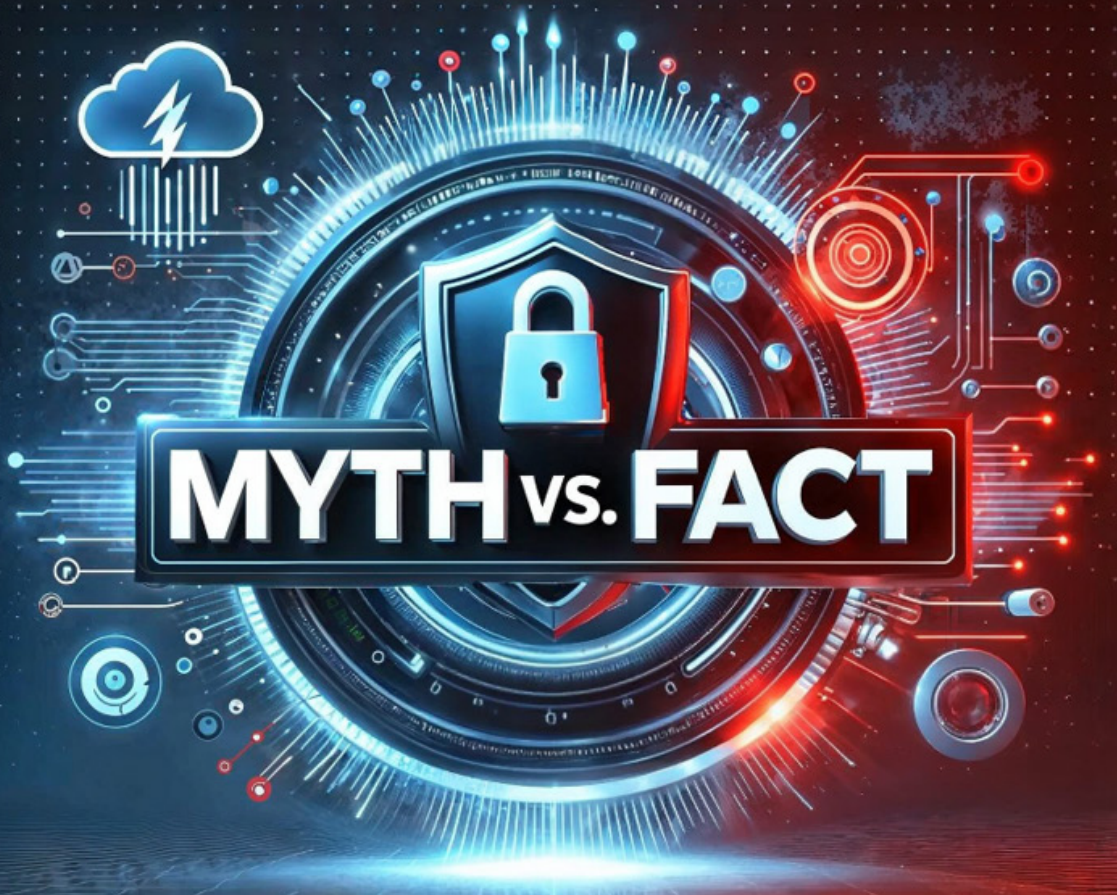
المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER

A digital graphic overlay featuring glowing blue lines, dots, and a circuit-like pattern, suggesting a network or data flow. The background is a city skyline at dusk, with prominent skyscrapers and a body of water in the foreground. The text "Cybersecurity Is a Business Enabler" is displayed in white, bold, sans-serif font in the lower-left corner.

Cybersecurity Is a Business Enabler

06

Addressing Common Cybersecurity Misconceptions



Understanding common cybersecurity misconceptions is vital for building a robust cybersecurity strategy. By dispelling these myths, micro, small, and medium enterprises (MSMEs) can avoid costly mistakes and ensure they are better prepared to defend against evolving cyber threats. Here are some widely held myths and the facts that should be considered when addressing cybersecurity.



Myth 1:
**An organization's data
isn't valuable enough to
be targeted.**

Many believe that small businesses are not attractive to cybercriminals. However, every organization holds valuable data, such as payment information, customer records, and intellectual property, which can be exploited by cybercriminals. SMEs are often targeted because they may not have strong security measures in place, making them easy targets for opportunistic attackers.



Myth 2: **Cybersecurity is too expensive for small businesses.**

It is a misconception that cybersecurity is unaffordable for small businesses. The cost of a cyberattack—whether from financial loss, reputational damage, or fines—can far exceed the cost of basic security measures. Basic tools like firewalls, encryption, and multi-factor authentication (MFA) are affordable and provide essential protection for businesses.



Myth 4: **Cybersecurity risks only come from external sources.**

While many cyberattacks come from outside the organization, internal threats are just as significant. Employees or contractors with access to critical systems and sensitive data can unintentionally or intentionally cause harm. It is essential to manage internal risks by implementing proper access controls, security protocols, and regular employee training.



Myth 3: **Technology alone can solve cybersecurity problems.**

Technology is a key element in any cybersecurity strategy, but it is not the only solution. Employees play a crucial role in preventing security breaches. Human error, such as falling for phishing attacks or misplacing devices, is often the weak link in cybersecurity. A comprehensive approach that includes both technology and training is necessary to protect businesses effectively.



Myth 5: **Mobile devices are safe from viruses and malware.**

Mobile devices are frequently targeted by cybercriminals, often more so than traditional computers. They store sensitive information and can be easily exposed through inadequate security, such as unsecured apps or jailbreak devices. Mobile devices also face risks from theft or loss, which can lead to unauthorized access to company data.



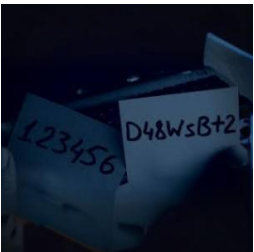
Myth 6: **Antivirus software alone is enough for cybersecurity.**

While antivirus software helps protect against known threats, it is not enough on its own to defend against advanced cyberattacks. Modern cyber threats like phishing and social engineering can bypass antivirus protections. A multi-layered security strategy, including firewalls, intrusion detection systems, and employee training, is essential to mitigate the risk of an attack.



Myth 8: **Cloud storage is always secure.**

Cloud storage is often perceived as inherently secure. While cloud providers implement strong security measures, businesses are still responsible for securing their data. Misconfigured cloud settings or insufficient access controls can lead to security vulnerabilities. Regularly auditing cloud security settings, encrypting sensitive data, and controlling access permissions are necessary to maintain cloud security.



Myth 7: **Strong passwords alone will keep us safe.**

Strong passwords are an important part of cybersecurity, but they are not a guarantee of protection. Cybercriminals can still break passwords using brute-force attacks or other methods. Additionally, human error, such as falling victim to phishing scams, can compromise passwords. Using multi-factor authentication (MFA) adds an additional layer of protection to secure access.

By addressing these common myths, micro, small, and medium enterprises (MSMEs) can better understand the importance of cybersecurity and implement effective strategies to protect their digital assets and ensure long-term business success.

07

Case Studies: Insights from Cybersecurity Incidents

As cyber threats become increasingly sophisticated, safeguarding sensitive data is imperative for businesses of all sizes. The following case studies highlight critical lessons learned from real-world breaches, providing small and medium-sized enterprises (SMEs) with insights to bolster their cybersecurity measures.

Case 01

Data-Wiping Malware Attack

In December 2021, a major oil company in the Gulf region was targeted by a cyberattack involving the “Dustman” data-wiping malware, designed to erase critical data, disrupt operations, and compromise system integrity. The attack was attributed to state-sponsored actors exploiting unpatched vulnerabilities and network security.

Key Takeaways:

1. Deploy Intrusion Detection and Prevention Systems (IDPS)

Implement both network-based intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS) to monitor traffic and detect threats in real-time. Integrate IDPS with Security Information and Event Management (SIEM) to centralize logging and automate alerts.

2. Establish Regular Data Backups and Incident

Adopt the 3-2-1 backup rule (three copies, two on different media, one offsite) to ensure business continuity. Protect backups by encrypting them, automate the backup process to make it easier, and perform regular tests to ensure the backups can be restored. Establish and maintain a comprehensive Incident Response Plan (IRP), ensuring readiness for rapid response during a breach.

A photograph of a large warehouse interior with high ceilings, industrial shelving units filled with cardboard boxes, and a forklift operator in the distance.

Case 02

Supply Chain Attack in 2024

In 2024, a sophisticated cyberattack targeted a governmental entity in the Gulf region using supply chain attack tactics. The attackers exploited vulnerabilities in third-party vendor systems to infiltrate the government's systems. This breach compromised the confidentiality, integrity, and availability of sensitive data, leading to severe operational disruptions and threats to citizen privacy.

Key Takeaways:

1. Enhance Vendor Risk Management

Implement a vendor risk management program that includes regular security assessments of third-party systems, especially those with access to critical infrastructure. This helps identify vulnerabilities before they can be exploited.

2. Implement Strong Access Control Measures

Identity and Access Management (IAM) controls access to critical systems, ensuring that only authorized users and devices can access sensitive data. Enforce least privilege access (PoLP), automate vendor access reviews, and integrate multi-factor authentication (MFA) to minimize risks.

A photograph of a server room with rows of server racks. A monitor in the foreground displays a red 'SYSTEM HACKED' warning over a world map.

Case 03

Cloud Data Breach in 2019

In 2019, a major data breach occurred at a financial technology company due to a vulnerability in its cloud infrastructure, exposing the personal data of over 100 million customers, including sensitive information such as Social Security numbers, credit scores, and bank account details. The breach remained undetected for months until the attacker publicly bragged about it online. Although the company quickly mitigated the damage, the incident led to significant reputational harm and a loss of customer trust.

Key Takeaways:

1. Implement Strong Access Control and Permissions

Enforce strict controls for sensitive data by applying the principle of least privilege (PoLP), granting access only when necessary.

2. Automate Security Monitoring

Use automated tools to continuously monitor cloud environments, detect unusual activity, and respond quickly to misconfigurations or unauthorized access.

Case 04

Data Breach Due to Weak VPN Security and BYOD Policies in 2022

In 2022, a small digital marketing company with limited IT resources experienced a data breach due to weak virtual private network (VPN) security and inadequate bring your own device (BYOD) policies. The company allowed employees to access systems remotely via VPN, but the use of personal devices with insufficient security created significant vulnerabilities.

The company relied on an outdated VPN protocol that wasn't regularly updated. Attackers exploited these weaknesses, including a compromised employee device that lacked proper antivirus updates. Through a phishing attack, they stole VPN credentials, accessed the company's internal network, and extracted sensitive client data, including payment details and business communications.

Key Takeaways:

1. Strengthen VPN Security and Monitoring

Upgrade to secure VPN protocols such as OpenVPN or IKEv2/IPSec and enforce continuous monitoring to detect unusual activity. Set up real-time alerts to respond quickly to unauthorized access attempts and prevent credential-based attacks.

2. Enforce Strong BYOD Security and Access Controls

Require data encryption and ensure regular updates on personal devices. Use cost-effective Mobile Device Management (MDM) solutions to enforce security policies. Apply the principle of least privilege (PoLP) to restrict access based on roles, ensuring employees can only access the data they need.

08

Cyber Threats and Risk Assessment for MSMEs

Micro, small, and medium enterprises (MSMEs) are increasingly targeted by cybercriminals due to their limited resources, lower investment in cybersecurity, and reliance on digital operations.

Understanding the threat landscape and conducting regular risk assessments are critical first steps toward building cyber resilience.

Key Cyber Threats Facing MSMEs



Phishing and Social Engineering

Deceptive emails or messages that trick employees into revealing sensitive information.



Ransomware

Malware that encrypts critical business data, demanding a ransom payment for its release.



Insider Threats

Risks posed by current or former employees and third-party vendors with access to systems.



Data Breaches

Unauthorized access leading to the theft or exposure of customer or business data.



Supply Chain Attacks

Exploitation of less-secure suppliers or service providers to gain access to the MSME's systems.



Denial of Service (DoS) Attacks

Overloading systems or websites to disrupt business operations.

The Importance of Risk Assessment

Conducting regular cybersecurity risk assessments helps micro, small, and medium enterprises (MSMEs):



Identify and prioritize critical assets.



Implement effective mitigation strategies.



Understand vulnerabilities and likely attack vectors.



Allocate resources efficiently toward the highest risks.

A Practical Risk Assessment Approach for MSMEs

MSMEs can adopt a simple yet effective method to assess cybersecurity risks:

1. Identify Assets

List digital and physical assets (e.g., servers, customer data, intellectual property).

2. Identify Threats and Vulnerabilities

Understand how assets might be threatened and what weaknesses exist.

3. Assess Impact and Likelihood

Determine the potential business impact and the likelihood of different threats.

4. Prioritize Risks

Focus on the highest-risk areas first.

5. Implement Controls

Apply appropriate cybersecurity controls and mitigation measures.

6. Monitor and Review

Regularly review risk profiles and adjust security strategies based on evolving threats.

Tip:

MSMEs can leverage international frameworks such as the National Institute of Standards and Technology (NIST) cybersecurity framework or ISO/IEC 27005 for guidance, adapting them into simplified forms suitable for their business scale.



09

Cybersecurity Maturity Model for MSMEs

Building cybersecurity capabilities is not a one-time effort but an evolving process. To help micro, small, and medium enterprises (MSMEs) progress systematically, this Cybersecurity Maturity Model provides three practical stages for growth.

Each stage allows businesses of different sizes and capabilities to adopt cybersecurity practices aligned with their operational needs and resources.



Level 1 Basic Cyber Hygiene

Essential protection in place. Reactive posture to cybersecurity threats.

Key Actions



Install antivirus software and firewalls



Regularly back up critical data



Enable multi-factor authentication (MFA)



Conduct basic employee cybersecurity training

Level 2 Managed Cybersecurity

Proactive threat management with documented processes and regular reviews.

Key Actions



Develop cybersecurity policies and procedures



Implement regular vulnerability scanning



Formalize risk assessment and incident response planning



Train employees on advanced threat recognition (e.g., phishing simulations)

Level 3 Advanced Cyber Resilience

Cybersecurity fully embedded into business strategy and culture. Continuous improvement driven by leadership.

Key Actions



Integrate security into all technology deployments "security by design"



Participate in threat intelligence sharing networks



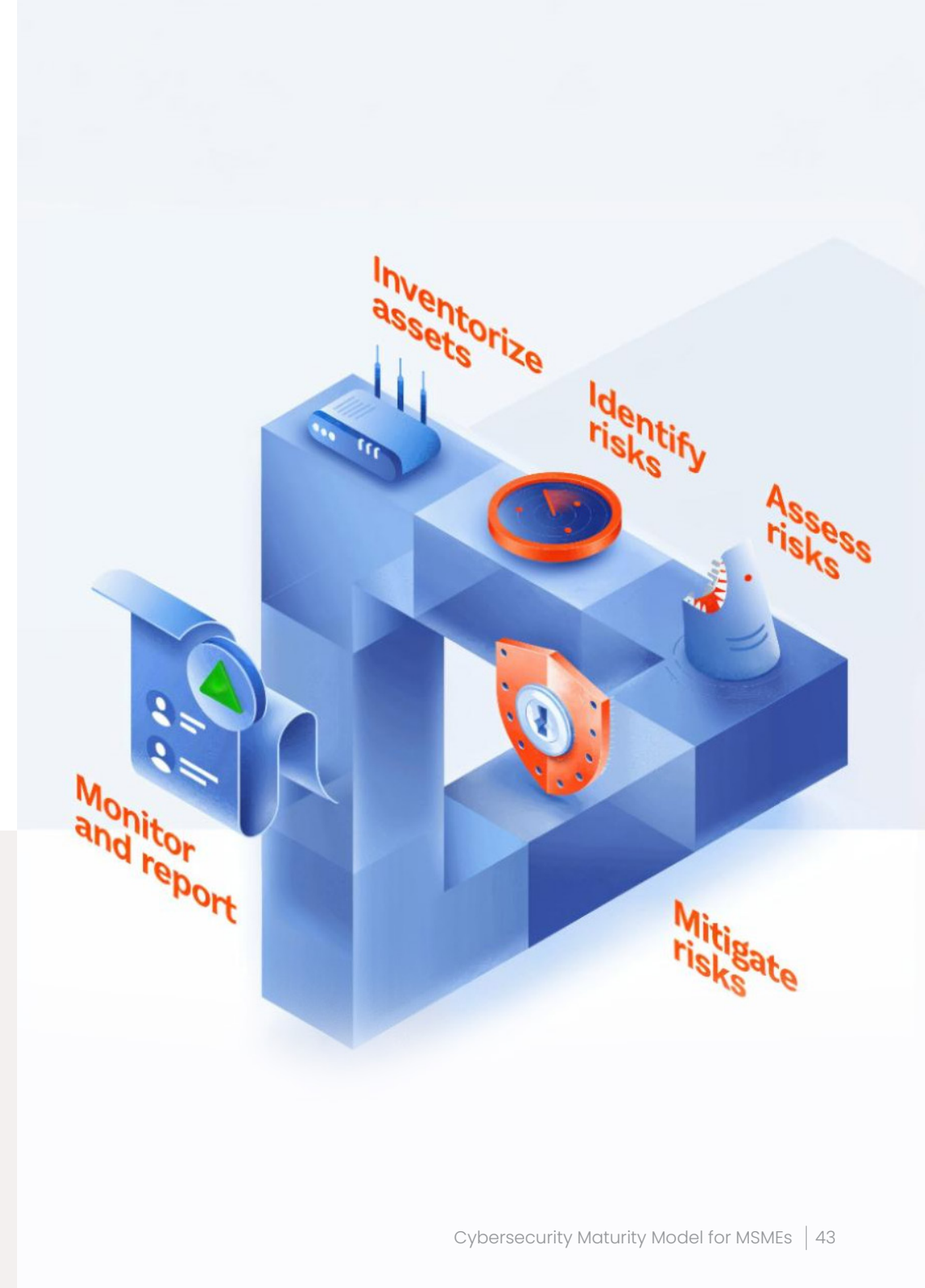
Conduct penetration testing and audits



Appoint or outsource a cybersecurity officer or function

Note:

Micro, small, and medium enterprises (MSMEs) should aim to gradually advance through these stages based on their resources, risk appetite, and operational needs. Even reaching Level 2 significantly improves resilience against the most common cyber threats.



10

The SMESEC Framework: 10 Strategic Steps to Strengthen Cybersecurity for Small and Medium Enterprises (SMEs)

01

Establish Cybersecurity Leadership and Risk Management

- Endorse cybersecurity at the highest management level.
- Develop a comprehensive cybersecurity risk management policy.
- Regularly assess cybersecurity risks and mitigation strategies.

02

Strengthen Access Controls and Authentication

- Apply the principle of least privilege (PoLP) for user access.
- Enforce multi-factor authentication (MFA) for critical systems.
- Regularly review access rights.

03

Secure Systems and Applications

- Ensure all devices and software are updated with the latest patches.
- Deploy antivirus and endpoint protection solutions.
- Remove or disable unnecessary services.

04

Defend Against Malware and Phishing Attacks

- Train employees to recognize and report phishing.
- Use email security filters.
- Deploy anti-malware solutions on all devices.

05 Protect Network Infrastructure

- Implement firewalls and intrusion detection systems (IDS).
- Use virtual private networks (VPNs) for remote access.
- Segment networks to isolate critical assets.

06 Backup and Secure Data

- Conduct regular, automated backups.
- Encrypt backup data and store it securely offsite.
- Test backup restoration procedures periodically.

07 Develop and Test an Incident Response Plan (IRP)

- Prepare a response plan tailored to your business size.
- Define communication procedures for incidents.
- Conduct regular drills to test incident readiness.

08 Promote a Cybersecurity-Aware Culture

- Conduct frequent cybersecurity awareness training.
- Update employees on emerging threats and prevention techniques.
- Encourage reporting of suspicious activity.

09 Secure the Supply Chain

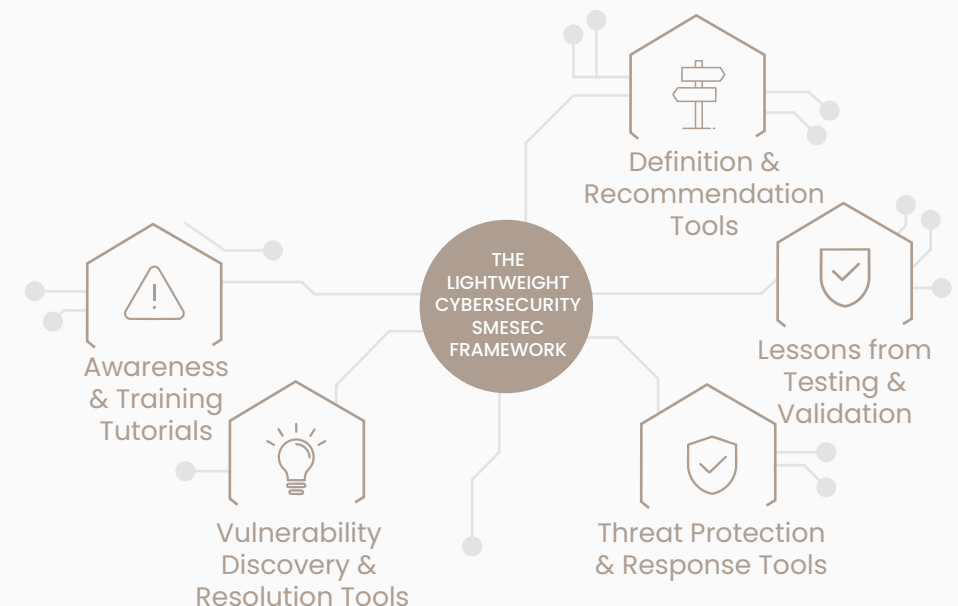
- Assess the cybersecurity practices of key vendors.
- Include cybersecurity requirements in contracts.
- Continuously monitor supply chain partners for risks.

10 Audit, and Improve

- Continuously monitor IT systems for threats.
- Conduct regular security audits.
- Update policies and controls in response to new threats.

The SMESEC framework

Small and medium enterprise security (SMESEC) is a lightweight cybersecurity framework for protecting SMEs against cyber threats. As an SME, you find vulnerabilities and address them with simple tutorials, tools, and lessons learned — all by yourself.



Global Best Practices for MSME Cybersecurity

Below is a conceptual table showing how major international cybersecurity frameworks align to support micro, small, and medium enterprises (MSMEs):

Framework	Key Focus Areas	Framework	Key Focus Areas
01 Cyber Resilience Playbook – WEF	<ul style="list-style-type: none">○ Establish a risk management culture○ Build resilience into supply chains	03 Small Business Cybersecurity Corner – NIST	<ul style="list-style-type: none">○ Emphasize the five cybersecurity functions: identify, protect, detect, respond, and recover.○ Provide a tailored cybersecurity checklist for SMEs
02 Cyber Essentials Framework – UK NCSC	<ul style="list-style-type: none">○ Ensure a secure internet connection○ Secure devices and software○ Control access to data and services○ Protect against viruses and malware○ Update software regularly	04 Global Cybersecurity Agenda – ITU	<ul style="list-style-type: none">○ Develop legal and regulatory frameworks○ Strengthen organizational structures○ Build national and international cooperation

On an Ending Note

“Empower Your Cybersecurity Journey”

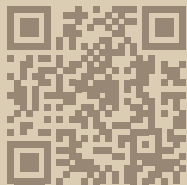
Micro, small, and medium enterprises (MSMEs) play a vital role in Bahrain’s economic growth and innovation. As they increasingly embrace digital technologies, strengthening cybersecurity practices is essential to safeguard their operations, customer trust, and long-term success.

This guidebook provides strategic guidance tailored for MSMEs to enhance their cybersecurity resilience in alignment with Bahrain’s Economic Vision 2030 and global best practices.

Effective cybersecurity is not achieved in isolation. MSMEs are encouraged to collaborate closely with national and sectoral cybersecurity entities, such as the National Cyber Security Center (NCSC) and other relevant authorities. In the event of a cyber incident, prompt reporting to these entities ensures access to expert support, rapid response capabilities, and collective defense mechanisms.

By adopting a proactive cybersecurity approach and engaging with trusted national resources, MSMEs contribute not only to their own business resilience but also to Bahrain’s overarching digital security ecosystem.

Stay Secure.
Stay Resilient.



ncscbh



ncsc_bh



www.ncsc.gov.bh